IMPLEMENTING DOD/OSD IA T&E POLICY FOR MULTI-SERVICE INFORMATION SYSTEMS

Abid Khan

April 23, 2009

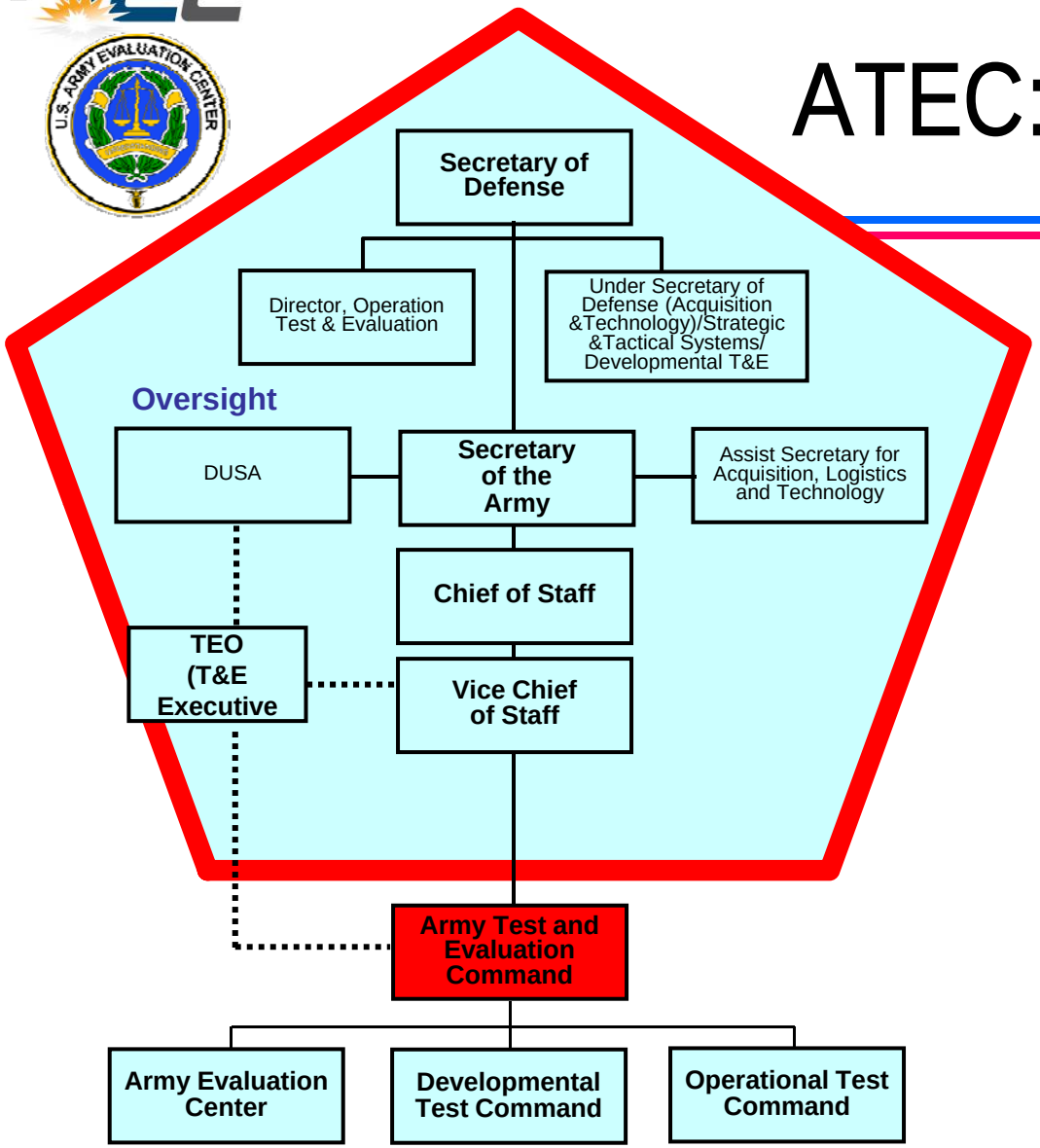
Army Proven
Battle Ready

Army Evaluation Center

AGENDA

- ATEC: HOW WE FIT
- Information Warfare and Impact to DoD Information Systems
- OSD Information Assurance Policies
- ATEC's T&E Methodology
- Lessons Learned
- Contact
- SUMMARY

ATEC: HOW WE FIT



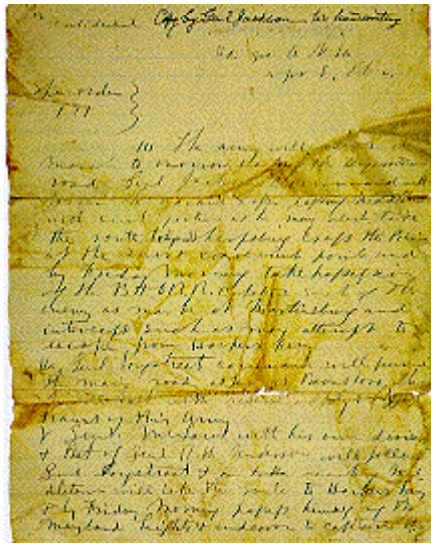
ATEC Customers:

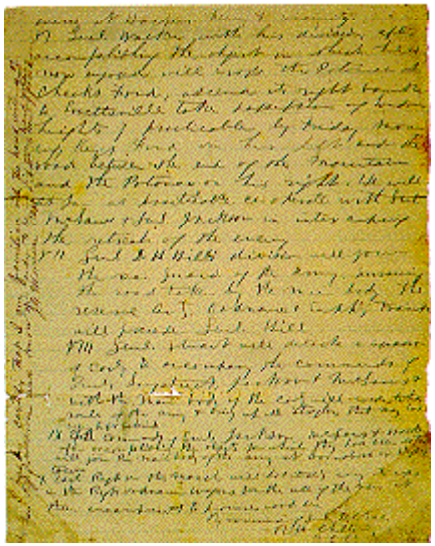
- Congress
- The Warfighter
- Army Decision-Makers
- Program Managers
- Other Government Agencies
- Defense Contractors

INFORMATION WARFARE

Information Warfare is a **form of conflict** in which the objective is to capture, degrade, or destroy the enemy's means of gathering, analyzing, and distributing **data**, particularly data regarding the enemy's **armed forces**.

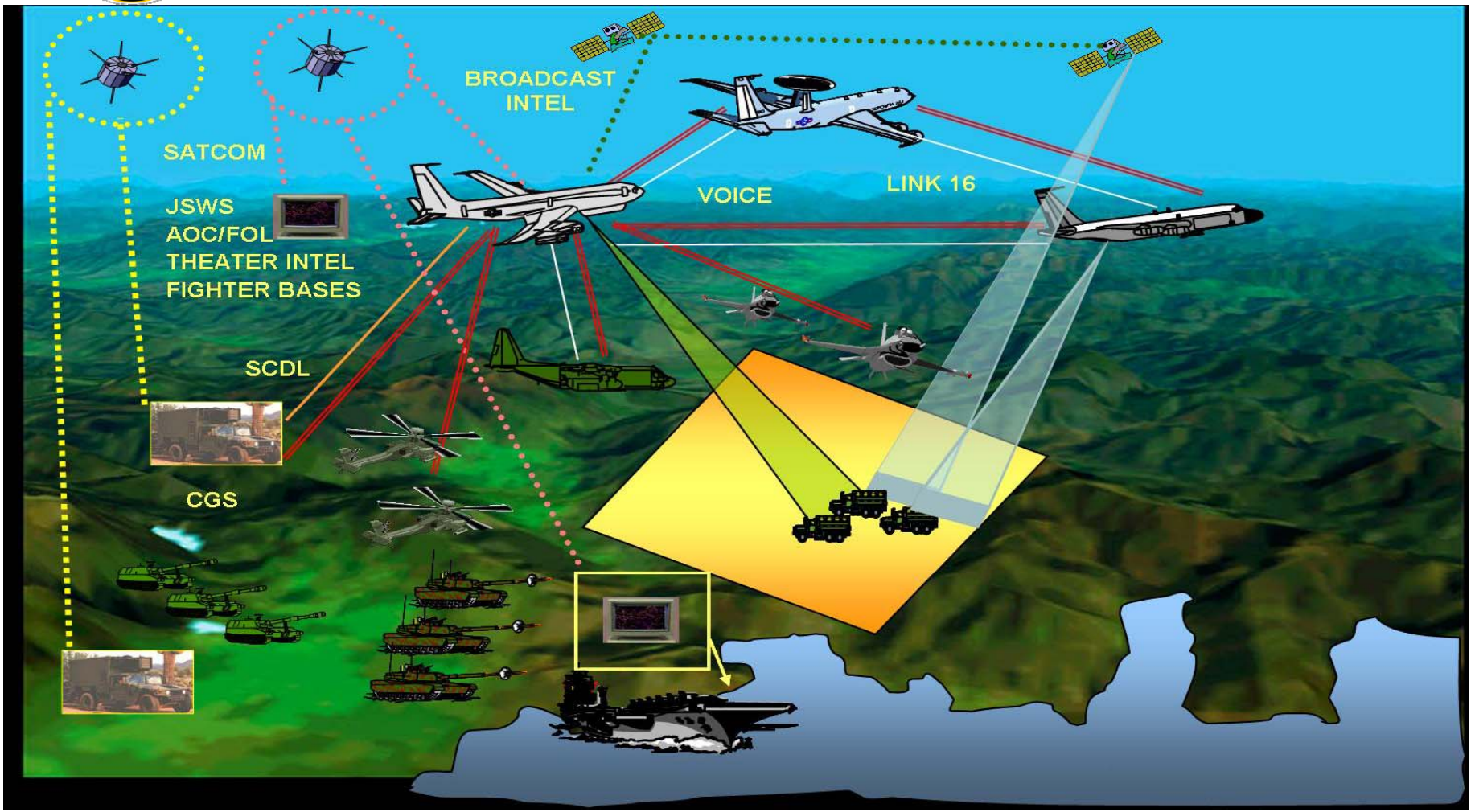
Information Warfare Example: THE LOST ORDER





INFORMATION WARFARE CHANGED THE COURSE OF THE CIVIL WAR AND ULTIMATELY LED TO THE DOWNFALL OF THE CONFEDERACY.

NETWORK-CENTRIC WARFARE



INFORMATION ASSURANCE

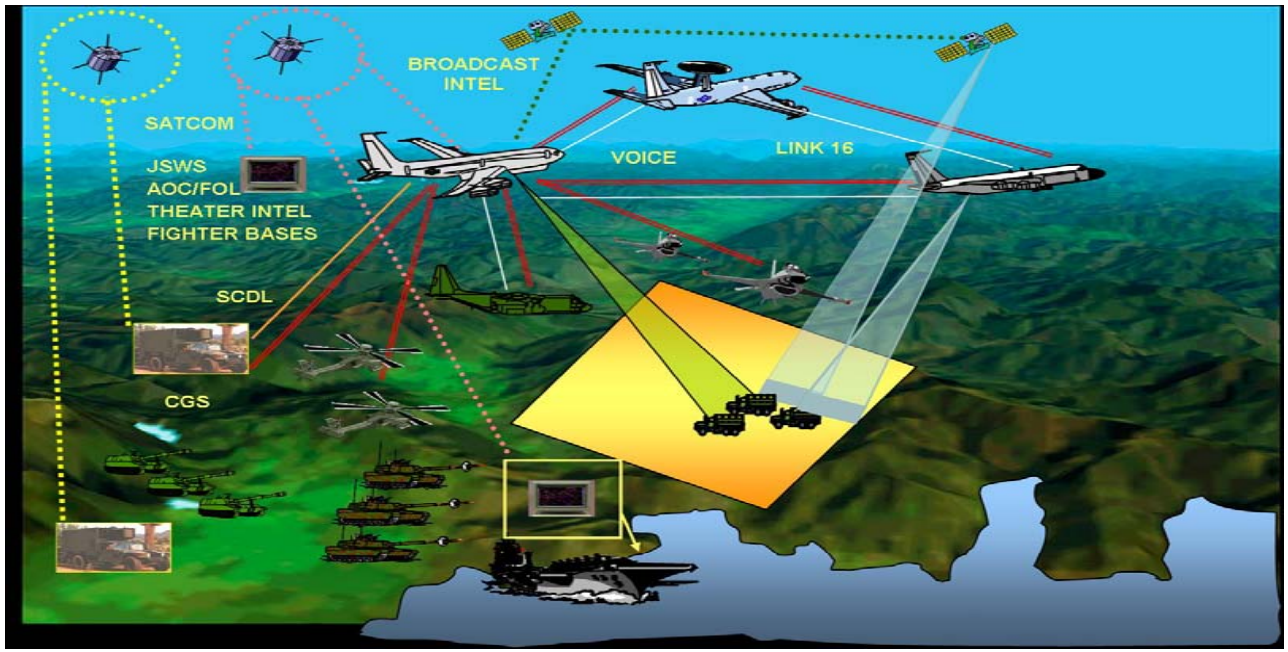
Information Assurance (IA) consists of "**measures that protect and defend information** and information systems by ensuring their *availability, integrity, authentication, confidentiality, and non-repudiation*. This includes **providing for the restoration** of information systems by incorporating protection, detection, and reaction capabilities." (*Department of Defense Directive 8500.1*)

- DoDD 8500.1 – Information Assurance
- DoDI 8500.2 – Information Assurance implementation
- DoDI 8510.01 – Certification & Accreditation (DIACAP)

IA IN OPERATIONAL MODE

- IA posture of combined system in a fully operational mode can be very different then a stand-alone system.

- In an operational environment, Soldiers/the system can demonstrate ability to defend the network under attack.



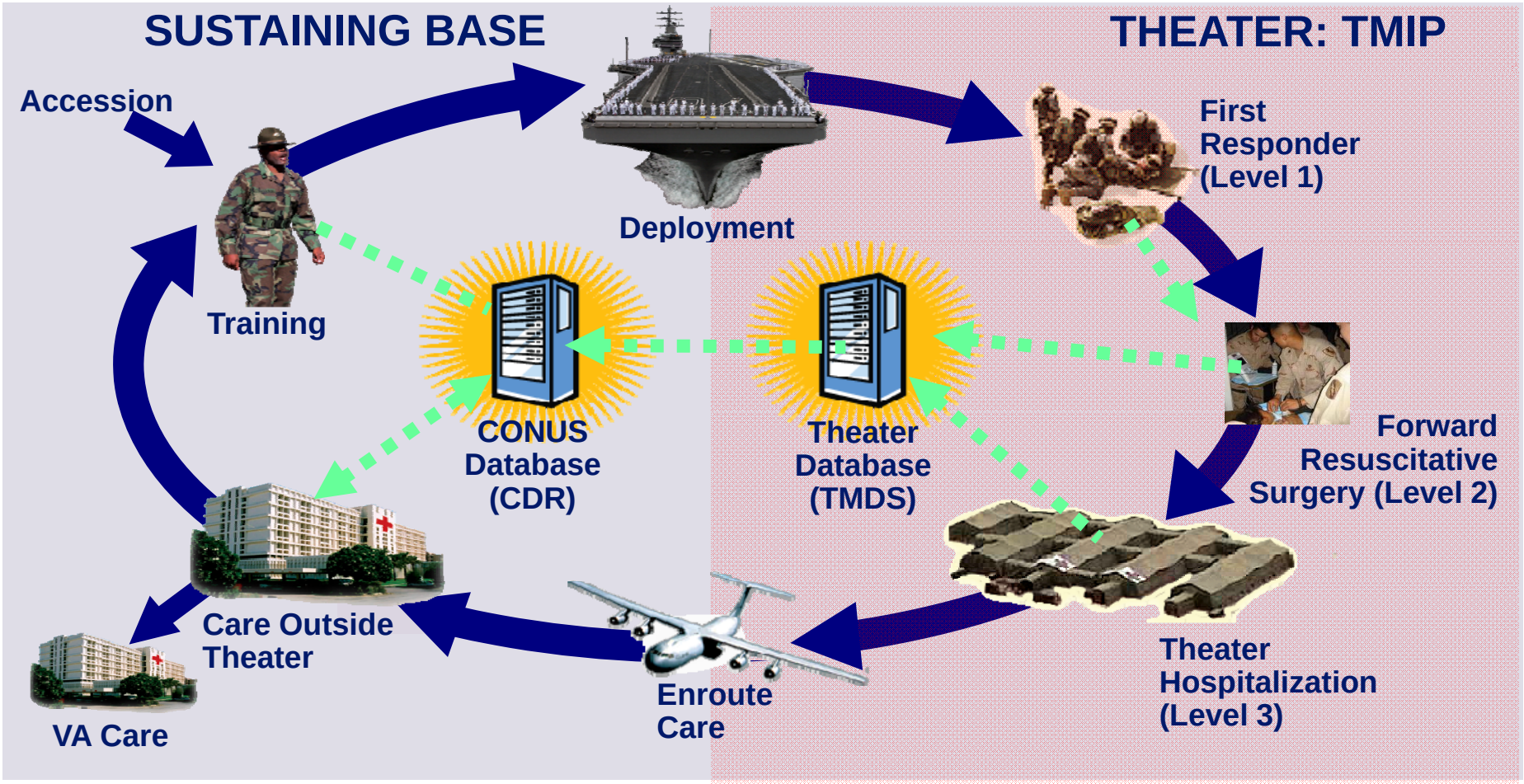
OSD's IA POLICY OVERVIEW

- Policy Steps:
  - Step 1: Determine Applicability
  - Step 2: Initial IA Review
  - Step 3: OT&E IA Risk Assessment
  - Step 4: Operational Vulnerability Evaluation
  - Step 5: Protection, Detection, Reaction, and Restoration Operational Evaluation (PDRR)
  - Step 6: COOP Evaluation

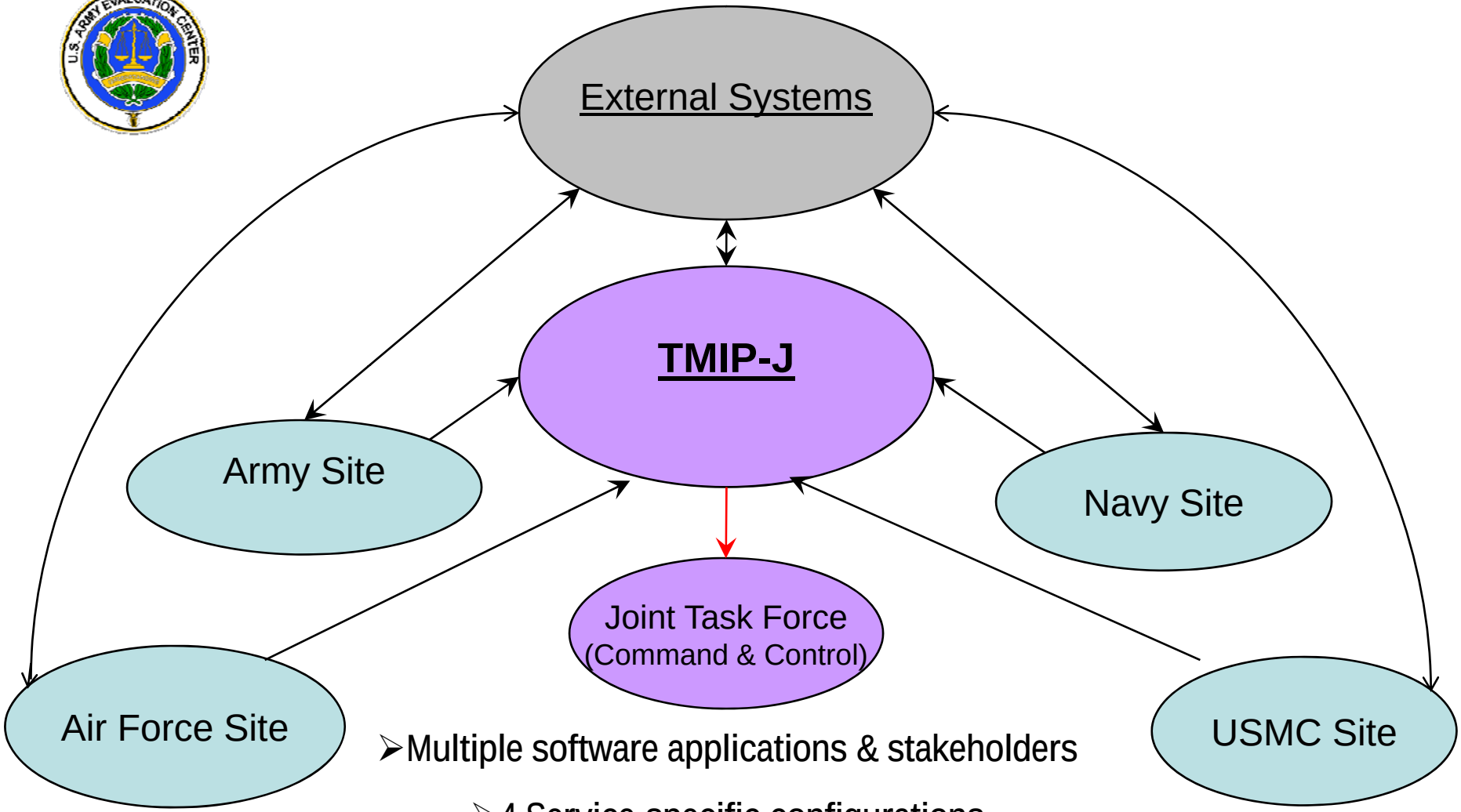
TMIP-J SYSTEM OVERVIEW

- Theater Medical Information Program – Joint /w DOT&E over site.
- Multi-Service system-of-systems that automates healthcare documentation, medical command and control reporting, and medical logistics in a combat theater environment.
- Resides on service-specific systems.
- ATEC is the lead Operational Test Agency.

TMIP-J'S ROLE IN THE CONTINUUM OF MEDICAL CARE



TMIP-J COMPLEXITY



- Multiple software applications & stakeholders
- 4 Service-specific configurations
- 5 Program Managers
- Distributed Testing

TMIP-J's IA TEST IMPLEMENTATION CHALLENGES

- Rigid Timetable
- Distributed Testing
- Diverse viewpoints
- No unity of effort
- 5 Program Managers & multiple stakeholders
- Service-specific medical software & hardware
- Software release agreements

SOLUTION: ATEC's LETTER OF INSTRUCTION

LETTER OF INSTRUCTION

- Establishes IA testing procedures to be used during VA & PDRR.
- Establishes responsibilities and defines Memorandum Of Agreement needed to accomplish the mission.
- Sets the Rules of Engagement for VA & PDRR teams.
- Agreement between all key stakeholders.
- Generated and coordinated by lead OTA.

THE KEY TO A SUCCESSFUL MULTI-SERVICE IA EVENT IS THE LETTER OF INSTRUCTION.

VA & PDRR TEAM SELECTION

- Experience & Expertise
- Certification (PDRR)
- Availability
- Logistics
- Cost
- Training
- Data Collectors
- Reporting

APPROPRIATE VA & PDRR SELECTION IS A KEY STEP TOWARDS SUCCESSFUL IA TESTING.

VULNERABILITY ASSESSMENT MISCONCEPTIONS

- Leverage DIACAP results.
- Service-specific IA VA.
- Vulnerability Assessment team is unnecessary & costly.

AN INDEPENDENT VA TEAM PROVIDES A CONSISTENT AND THOROUGH APPROACH TO FINDING SYSTEM VULNERABILITIES. IN THE LONG RUN, THE VA TEAM PAYS FOR ITSELF.

IA OT&E PLANNING

- Cooperation from the Services
- Service-specific inquiries
- DAA approval of PDRR testing
- Mitigations prior to PDRR

IA OT&E EXECUTION

- Exercise overall coordination for VA & PDRR teams during testing activities.
- Communicate IA test status to all stakeholders during and after testing.
- Act as the central POC for resolution of IA testing issues.
- Attend entry and exit briefings for key leaders at respective test sites.

VALIDATION OF FINDINGS

- Only a select, highly technical group (e.g. system admin.) can validate VA & PDRR findings

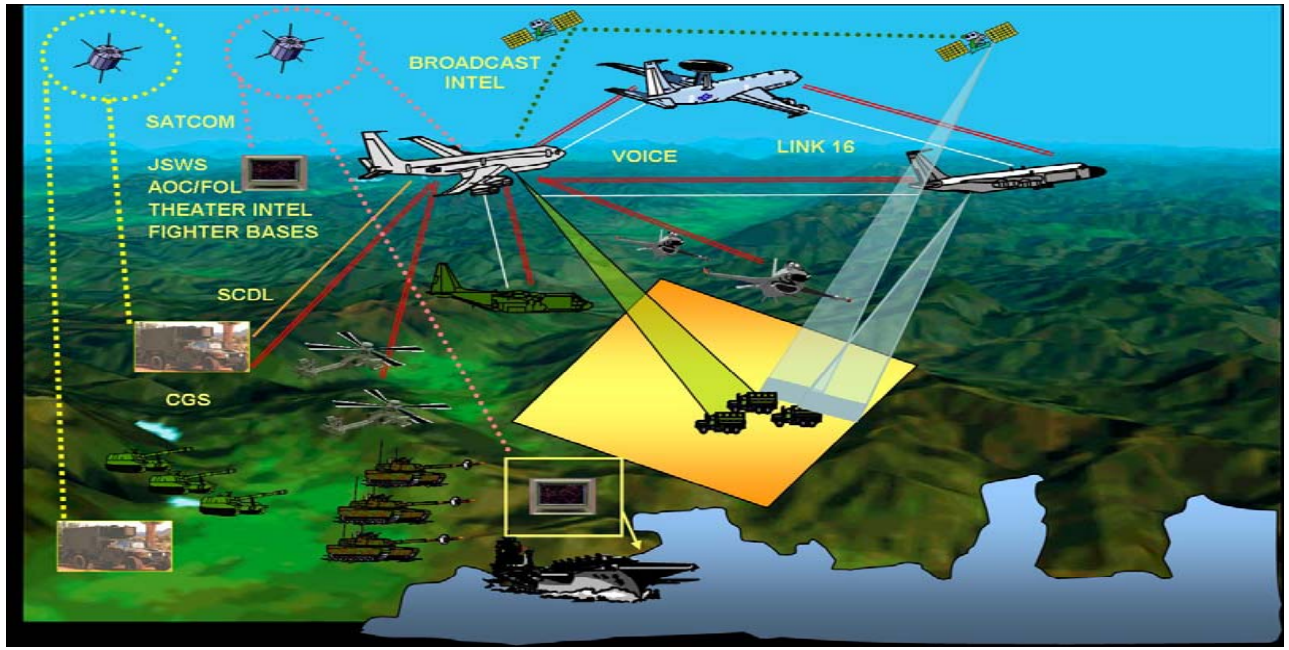
- Validation occurs after daily VA / PDRR updates and after mission out brief.

LESSONS LEARNED: PLANNING

- Ensure that IA is integrated into T&E strategy.
- Coordinate LOI for VA and PDRR testing as early as possible.
- Ensure VA & PDRR teams are prepared for mission.
- Maintain contact with alternate Information Assurance test teams.
- Work closely and coordinate with PM IA Managers and other IA stakeholders.

LESSONS LEARNED: TEST EXECUTION

- Create test cases to evaluate system's defensive posture; Protection ≠ Detection
- Generate insider threat scenarios.
- Conduct penetration testing as close as possible to wartime information operations.



HARDEN SOFTWARE SYSTEMS

- Define Patch Management Responsibilities
- Periodically test IAVA
- Document & test COOP
- Test alternate site functionality
- Monitor Account Management Process

SUMMARY

- ATEC has demonstrated the capability to test and evaluate the IA posture of complex, Multi-Service information systems.
- The Letter Of Instruction is a tool for planning, coordinating and implementing successful Multi-Service IA test events.
- Effective information assurance is the best defense against information warfare.

CONTACT

Abid Khan

410-306-1263, DSN 458-1263

Email: Abid.Khan@us.army.mil

Michael Brown

(703) 845-3871, DSN 458-3871

Michael.L.Brown7@us.army.mil

QUESTIONS?

ACRONYMS

- ACAT 1AM – Acquisition Category 1 for Major Automated Information Systems
- ATEC – Army Test and Evaluation Command
- COOP – Continuity of Operations Plan
- DAA – Designated Approving Authority
- DIACAP – DOD Information Assurance Certification and Accreditation Process
- DoD – Department of Defense
- IA – Information Assurance
- IAVA - Information Assurance Vulnerability Assessment
- LOI – Letter of Instruction
- OSD – Office of Secretary of Defense
- OTA – Operational Test Agency
- OT&E – Operational Test & Evaluation
- PDRR – Protect Detect React Restore
- PM – Program Manager
- T&E – Test & Evaluation
- VA – Vulnerability Assessment